REMARKS

Claims 1-19 were currently pending in the patent application. By this amendment, Applicants cancel Claim 16. Claims 1-15 and 17-19 remain in the application. The Examiner has objected to Claim 1 for an informality; has rejected Claim 16 as being indefinite; has rejected Claim 19 as indefinite; has rejected Claims 1-5, 8, 11-14, and 16-19 under 35 USC 102 as anticipated by Jakubowski; and, has rejected Claims 6-7 and 9-10 as unpatentable over Jakubowski in view of Bender. The Examiner has also indicated that Claim 15 would be allowable if rewritten into independent format. In light of the amendments presented herein, and based on the arguments presented below, Applicants believe that all of the claims are allowable over the cited art.

With regard to Claim 1, Applicants have corrected the informality by deleting the ";". With regard to Claim 16, Applicants have canceled the claim. With regard to Claim 19, Applicants have amended the preamble to replace the indefinite language.

The present application teaches and claims a system, method and program storage device for uniquely authenticating each replication of a plurality of soft-copy documents forming a group, comprising the steps of

dynamically selecting one soft-copy document out of said group to become a carrier for an authentication code aimed at protecting the group, concatenating the plurality of soft-copy documents, wherein the concatenating includes the step of using a canonical form of the selected soft-copy document; computing an authentication code from the concatenated plurality of soft-copy documents and a predetermined key; generating a random number; and creating the carrier by combining the random number and the authentication code and marking the selected soft-copy document. By dynamically selecting one of the documents to be the carrier of the random number and authentication code, the present invention does not permit easy locating of the authenticating information at a predefined portion of the replication. In addition, by concatenating all of the soft copy documents, or all with the exception of the selected soft-copy document as recited in Claim 2, and then computing the authentication code from a key and the concatenated documents, the present invention prevents easy recognition of the encoded material.

The Examiner has cited the Jakubowski patent against all of the claims. The Jakubowski patent is directed to a system and method for providing secure encryption of a single plaintext message for transmission. During

encryption of a plaintext message, Jakubowski generates an intermediate stream including a MAC, wherein the MAC is defined as a predefined portion (i.e., two successive blocks) of the encoded message. The MAC is then encrypted and inserted into a predefined portion of the encrypted message. Throughout the patent, Jakubowski refers to the highest order two blocks as the portion of the stream for the MAC (see, for example, 449 and 452 of Fig. 4A and block 540 of Fig. 5). Once the MAC has been encrypted and inserted, the remainder of the message is generated including the encrypted message and a predefined variation which corresponds to the encrypted MAC. The resulting message, therefore, comprises some transformed message blocks, the encrypted MAC, and the remainder of the transformed message blocks with the encrypted MAC components spread throughout the remainder of the message. Upon receipt of a message in Jakubowski, the encrypted MAC is located at the predefined location and is compared to the encrypted MAC information found extended throughout the remainder of the message. If the two sets of MAC information correspond, then it is assumed that the message has not been tampered with during transmission.

Applicants respectfully assert that the Jakubowski patent does not teach or suggest the invention as claimed.

Applicants first note that authenticating a replication of a group of soft-copy documents is not the same as or suggestive of encoding a single message for transmission. Jakubowski does not deal with a group of soft copy documents, but only with a single plaintext message which Jakubowski divides into message blocks.

Next, Applicants note that Jakubowski does not dynamically select one soft copy document to be a carrier for an authentication code. Jakubowski expressly teaches that an encrypted MAC is inserted into a predefined portion of the encrypted message. Jakubowski inserts the encrypted MAC in an predetermined location of a single message stream, whereas the present invention selects a soft copy document to be the carrier of an authentication code for a group of soft copy documents.

Applicants next note that Jakubowski does not concatenate a plurality of soft copy documents, wherein the concatenating includes the step of using a canonical form of the selected soft-copy document. What Jakubowski teaches is concatenating blocks of the intermediate bit stream of transformed message blocks and then designating the concatenated transformed message blocks as the MAC. Concatenating successive blocks of a single message is not the same as or suggestive of concatenating a plurality of

soft copy documents. Moreover, the present invention then uses the concatenated plurality of documents and a key to compute an authentication code. Jakubowski simply designates a couple of successive message blocks of a single message as the MAC and then encrypts the MAC.

Finally, Applicants respectfully assert that Jakubowski does not teach or suggest the step or means for creating a carrier by combining a random number and the computed authentication code and marking the selected soft copy document. Jakubowski inserts the encrypted MAC into a predetermined location in the message stream and then inserts components of the encrypted MAC into expected locations of the remainder stream. Jakubowski does not mark a selected soft copy document with a random number and an authentication code computed from concatenated documents and a key.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Jakubowski patent does not teach steps or means for uniquely authenticating each replication of a plurality of soft-copy documents; for selecting one soft-copy document out of said group to become a carrier for an authentication code; for concatenating the plurality of soft-copy

documents, said concatenating including the step of using a canonical form of said selected soft-copy document; for computing an authentication code from said concatenated plurality of soft-copy documents and a predetermined key; and, for generating a random number and creating the carrier by combining the random number and the authentication code and marking the selected soft-copy document, it cannot be maintained that Jakubowski anticipates the invention as set forth in the independent claims, Claims 1, 17 and 19, or the claims which depend therefrom and add further limitations thereto.

Applicants further assert that the Jakubowski patent does not obviate the invention as claimed, alone or in combination with the additionally-cited Bender article. The Bender article is cited for its teachings with regard to marking a plain text document by the insertion of blank spaces. Applicants first argue that one having skill in the relevant art would not be motivated to modify Jakubowski with Bender. If one were to modify Jakubowski with Bender, one would arrive at a Jakubowski system wherein the encrypted MAC would be comprised of blank spaces. Inserting a plurality of blank spaces into the transformed message at the two highest order blocks would result in a discontinuous message stream which would probably be rejected or ignored

as an interrupted transmission. Essentially, suggesting that Jakubowski utilize blank spaces for the MAC would render Jakubowski unworkable for its intended purpose. Applicants remind the Examiner that, under U.S. Patent Law, references cannot be considered combinable for obviousness purposes if the combination would result in an unworkable result. In order to combine references, there must be motivation to combine and some reasonable expectation of success (*In re Wilson*, 424 F. 2d 1382, U.S.P.Q. 494, (C.C.P.A. 1970)).

Applicants further assert that, even if one were motivated to combine the teachings of Jakubowski and Bender, the resulting system and method would not obviate the presently claimed invention. Since neither Jakubowski nor Bender teaches or suggests authenticating each replication of a plurality of soft-copy documents; selecting one soft-copy document out of said group to become a carrier for an authentication code; concatenating the plurality of soft-copy documents, said concatenating including the step of using a canonical form of said selected soft-copy document; computing an authentication code from said concatenated plurality of soft-copy documents and a predetermined key; or generating a random number and creating the carrier by combining the random number and the

authentication code and marking the selected soft-copy document, the combination would not yield the invention as claimed. Since not all of the claim features have been taught or suggested by the cited references, a *prima facie* case of obviousness has not been established (*In re Wilson*, 424 F. 2d 1382, 1385, U.S.P.Q. 494, 496 (C.C.P.A. 1970)).

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

F. I. Carro, et al

By: Anne V. Dougherty

Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910